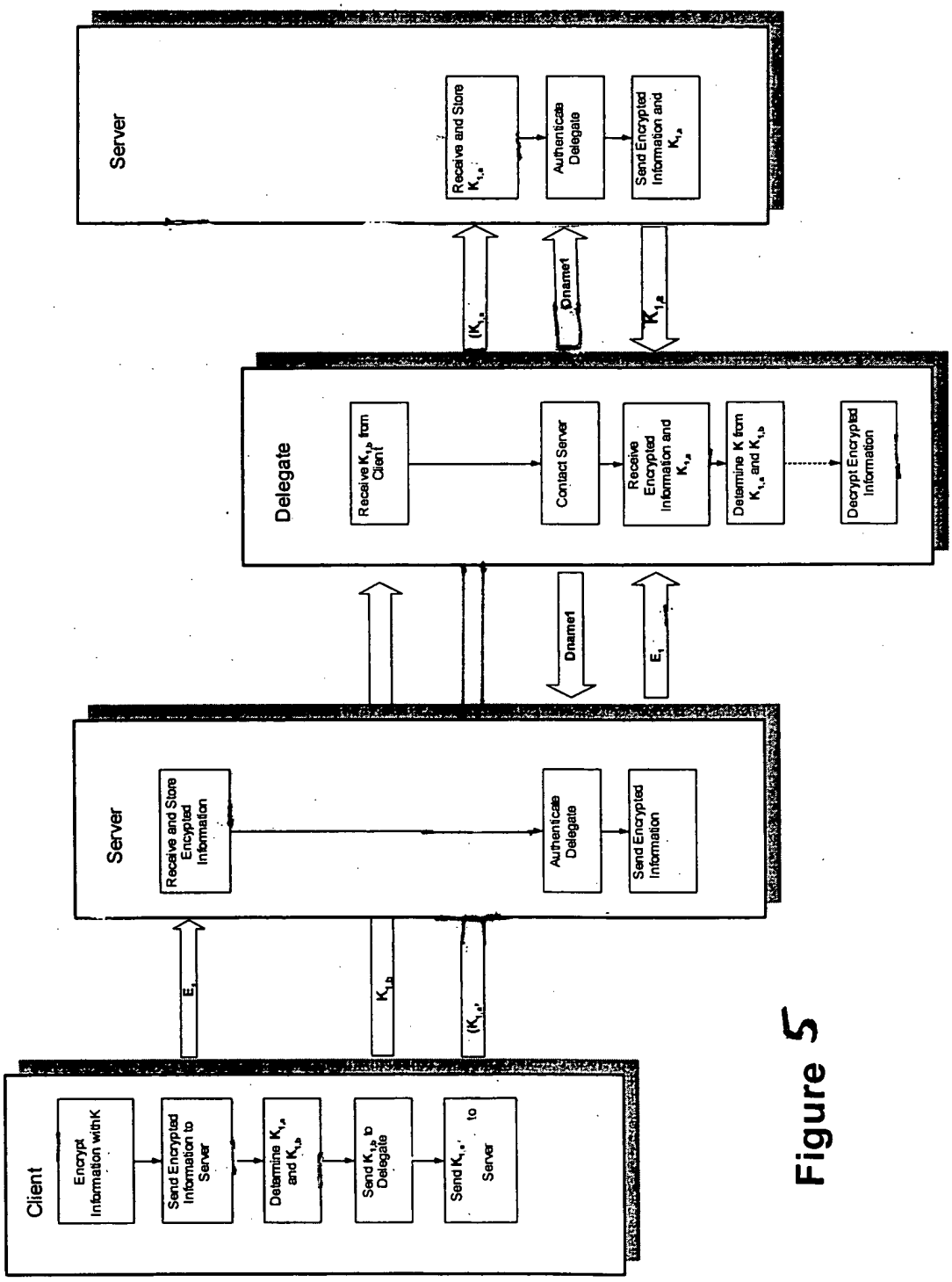
Server
Receive and Store $K_{1,a}$
Authenticate Delegate
Send Encrypted Information and $K_{1,a}$
$(K_{1,a}$
Dname1
$K_{1,a}$
Delegate
Receive $K_{1,b}$ from Client
Contact Server
Receive Encrypted Information and $K_{1,a}$
Determine K from $K_{1,a}$ and $K_{1,b}$
Decrypt Encrypted Information
Dname1
E_1
Server
Receive and Store Encypted Information
Authenticate Delegate
Send Encrypted Information
E_1
$K_{1,b}$
$(K_{1,a}$
Client
Encrypt Information with K
Send Encrypted Information to Server
Determine $K_{1,a}$ and $K_{1,b}$
Send $K_{1,b}$ to Delegate
Send $K_{1,a}$ to Server

Figure 5